

Appl. No. 09/785,722
Amdt. Dated April 19, 2006
Reply to Office Action of January 19, 2006

Docket No. CM04812H
Customer No. 22917

REMARKS/ARGUMENTS

Applicants have amended Claims 1, 16, 23 and 36 and have withdrawn Claims 42-48, 52-57, 59-71, 73-91 and 93 and 94 without prejudice. No new matter was added by these amendments. Claims 1-41 remain in this application. Moreover, Applicants further point out that the Examiner identified Claim 58 in the present Office Action as being pending. However, Claim 58 was cancelled in Applicants' amendment dated November 7, 2005.

The Examiner has restricted the claims in this application into Invention I (Group 1) comprising Claims 1-41, Invention II (Group 2) comprising Claims 42-48, 52-71, 73-91, 93 and 94 and Invention III (Group 3) comprising Claims 95-98. In accordance with the telephone conference between the Examiner and Applicants' attorney Valerie Davis on 01/10/06, Applicants confirm that they have elected Group 1 (Claims 1-41) without traverse.

The Examiner has rejected Claims 1-41 under 35 U.S.C. 103(a) as being unpatentable over "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000, in view of Roelofson ("TETRA Security"). Applicants traverse these rejections.

To establish a *prima facie* case of obviousness, and hence to find Claims 1-41 unpatentable under 35 U.S.C. § 103(a) over the combination of TETRA-2000 and Roelofson, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not be based upon applicant's disclosure. MPEP at § 2142. Applicants submit that the Examiner has not established a *prima facie* case of obviousness in this instance because the references when combined fail to teach or suggest all of the claim limitations.

Appl. No. 09/785,722
Amdt. Dated April 19, 2006
Reply to Office Action of January 19, 2006

Docket No. CM04812H
Customer No. 22917

More specifically, embodiments of the present invention as claimed in independent Claims 1, 16, 23 and 36 use a novel "intrakey" that is associated with a "pool of only infrastructure devices that are other than a mobile station", wherein the intrakey is "used only for encrypting key material that is distributed within the. . . pool [of devices]". As claimed, the intrakey is used for encrypting a "derived cipher key" that is "associated with securing air interface communications with [a] mobile station" (as recited in Claims 1 and 23) or that is used for "encrypting messages to the mobile station and decrypting messages from the mobile station" (as recited in Claims 16 and 36). Applicants submit that based on the following argument, the combined teachings of TETRA-2000 and Roelofson fail to teach or suggest the above-quoted limitations recited in independent Claims 1, 16, 23 and 36 and included by dependency in Claims 2-15, 17-22, 24-35 and 37-41.

The Examiner argues that "the intrakey is equivalent to either of Common Cipher Key (CCK), Group Cipher Key (GCK) or Static Cipher Key (SCK) when either of them is used to be associated with a particular group/location area" (Office Action dated January 19, 2006 at pages 5 and 7). Applicants disagree with this conclusion for a number of reasons. Applicants have recited in Claims 1, 16, 23 and 36 a novel intrakey defined therein by a number of features that none of the keys have, which are identified by the Examiner (i.e., CCK, GCK, SCK). These claimed features include that the intrakey is associated with a "pool of *only infrastructure devices that are other than a mobile station*", wherein the intrakey is "used *only for encrypting key material* that is distributed within the. . . pool [of devices]".

The CCK cannot be considered an intrakey because it is not associated with a pool of *only infrastructure devices that are other than a mobile station* and is not used *only for encrypting key material* distributed within the pool of devices. Instead in accordance with TETRA-2000 §4.2.3, the CCK "shall be used to give protection of voice, data, and signalling sequences between the infrastructure and an MS [mobile station] when using group addresses on the downlink" and is associated with a location area that includes mobile stations. The GCK cannot be considered an intrakey because it is not associated with a pool of *only infrastructure*

Appl. No. 09/785,722
Amdt. Dated April 19, 2006
Reply to Office Action of January 19, 2006

Docket No. CM04812H
Customer No. 22917

devices that are other than a mobile station and is not used *only for encrypting key material* distributed within the pool of devices. Instead in accordance with TETRA-2000 §4.2.2, the GCK is associated with a group of mobile stations and “may be used . . . to protect voice, data, and signalling sequences between the infrastructure and an MS when using group addresses”. Finally, the SCK cannot be considered an intrakey because it is not associated with a pool of *only infrastructure devices that are other than a mobile station* and is not used *only for encrypting key material* distributed within the pool of devices. Instead in accordance with TETRA-2000 §4.2.4, the SCK may be associated with a group of mobile stations and “may be used to protect voice, data, and signalling sequences between the infrastructure and a group-addressed MS”.

The Examiner correctly concedes that TETRA-2000 does not disclose using the intrakey to encrypt the derived cipher key as is recited in Claims 1, 16, 23 and 36 but argues that Roelofson includes teachings that read on such limitations. Applicants disagree. Roelofson does in fact mention the derived cipher key (or DCK) in its teachings (page 50, col. 2, 1st full paragraph). However, there is no further teaching or suggestion that this particular key can be or should be encrypted prior to being forwarded to a base station (Claims 1 and 23) or received by a base station (Claims 16 and 36). The only keys that Roelofson teaches may optionally be encrypted are the CCK and the GCK (neither of which are, of course, the DCK), and these two keys can, respectively, be encrypted by the DCK and a session encryption key (and not the intrakey as recited in Claims 1, 16, 23 and 36) before being forwarded to a mobile station (and not a base station as is recited in Claims 1, 16, 23 and 36) (*see* Roelofson pages 50-51).

Accordingly, Applicants believe that the subject application, as amended, is in condition for allowance. Such action is earnestly solicited by the Applicants and an early notice of allowance is respectfully requested.

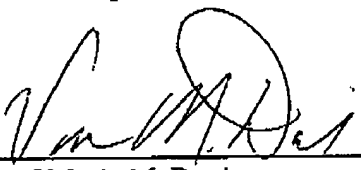
In the event that the Examiner deems the present application non-allowable, it is requested that the Examiner telephone the Applicants' attorney or agent at the number indicated below so that the prosecution of the present case may be advanced by the clarification of any continuing rejection.

Appl. No. 09/785,722
Amdt. Dated April 19, 2006
Reply to Office Action of January 19, 2006

Docket No. CM04812H
Customer No. 22917

Please charge any fees associated herewith, to Deposit Account No. 502117, Motorola,
Inc.

Respectfully submitted,


By: Valerie M. Davis

SEND CORRESPONDENCE TO:

Motorola, Inc.
Law Department
1303 E. Algonquin Road
Law Department
Schaumburg, IL 60196
Customer Number: 22917

Attorney of Record
Reg. No.: 50,203

Telephone: 847.576.6733
Fax No.: 847.576.0721